Amendments to the Claims:

A listing of the entire set of pending claims (including amendments to the claims, if any) is submitted herewith per 37 CFR 1.121. This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Previously presented) A method of linear transformation in a symmetric-key cipher comprising:

inputting block data into a processing apparatus;

creating a linear transformation matrix A with the processing apparatus by:

generating a binary [n,k,d] error-correcting code, represented by a generator matrix $G \in Z_2^{k \times n}$ in a form $G = (I_k \| B)$, with $B \in Z_2^{k \times (n-k)}$, where $k < n < 2k$, and d is the minimum distance of the binary error-correcting code;

shortening said error-correcting code; and

extending matrix B with 2k-n columns such that a resulting matrix C is non-singular, and deriving the linear transformation matrix A from matrix C; and

transforming the input block data into diffused output block data with the processing apparatus by using the linear transformation matrix A.

2. (Previously presented) A method as claimed in claim 1, wherein extending matrix B with 2k-n columns comprises:

in an iterative manner:

randomly generating 2k-n columns, each with k binary elements;

forming a test matrix consisting of the n-k columns of B and the 2k-n generated columns; and

checking whether the test matrix is non-singular, until a non-singular test matrix has been found; and

using the found test matrix as matrix C.

PAGE 4/12 * RCVD AT 8/14/2006 3:55:34 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/28 * DNIS:2738300 * CSID:703 5199802 * DURATION (mm-ss):01-56

3. (Previously presented) A method as claimed in claim 1, wherein the operation of deriving matrix A from matrix C comprises:

determining two permutation matrices $P_1, P_2 \in Z_2^{k \times k}$ such that all codewords in an [2k,k,d] error-correcting code, represented by the generator matrix (I_k || P_1 C P_2), have a predetermined multi-bit weight; and

using P_1 C P_2 as matrix A.

4. (Previously presented) A method as claimed in claim 3, wherein the input block data is m-bit sub-block data, and the processing apparatus executes a round function with an S-box layer with S-boxes operating on the m-bit sub-blocks data, and the minimum predetermined multi-bit weight over all non-zero codewords equals a predetermined m-bit weight.

5. (Previously presented) A method as claimed in claim 3, wherein determining the two permutation matrices P_1 and P_2 comprises iteratively generating the matrices in a random manner.

6. (Previously presented) A method as claimed in claim 1, wherein the input block data is 32-bit block data and wherein the operation of generating a [n,k,d] error-correcting code comprises:

generating a binary extended Bose-Chaudhuri-Hocquenghem (XBCH) [64,36,12] code; and

shortening the XBCH [64,36,12] code to a [60,32,12] XBCH code by deleting four rows.

7. (Previously presented) A computer program product stored on a computer readable medium, wherein the program product is operative to cause the a processor to perform the method of claim 1.

PAGE 5/12 * RCVD AT 8/14/2006 3:55:34 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/28 * DNIS:2738300 * CSID:703 5199802 * DURATION (mm-ss):01-56

8. (Previously presented) A system for cryptographically converting an input data block into an output data block, the input data blocks comprising n data bits, the system comprising:

an input for receiving the input data block;

a storage for storing a linear transformation matrix A created by:

generating a binary [n,k,d] error-correcting code, represented by a generator matrix $G \in Z_2^{k \times n}$ in a form $G = (I_k \| B)$, with $B \in Z_2^{k \times (n-k)}$, where $k < n < 2k$, and d is the minimum distance of the binary error-correcting code;

shortening said error-correcting code; and

extending matrix B with 2k-n columns such that a resulting matrix C is non-singular, and deriving the linear transformation matrix A from matrix C;

a cryptographic processor performing a linear transformation on the input data block or a derivative of the input data block using the linear transformation matrix A; and

an output for outputting the processed input data block.

9-10. (cancelled)

11. (Previously presented) A system as claimed in claim 8, wherein extending matrix B with 2k-n columns comprises:

in an iterative manner:

randomly generating 2k-n columns, each with k binary elements;

forming a test matrix consisting of the n-k columns of B and the 2k-n generated columns; and

checking whether the test matrix is non-singular, until a non-singular test matrix has been found; and

using the found test matrix as matrix C.

PAGE 6/12 * RCVD AT 8/14/2006 3:55:34 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/28 * DNIS:2738300 * CSID:703 5199802 * DURATION (mm-ss):01-56

12. (Previously presented) A system as claimed in claim 8, wherein the operation of deriving matrix A from matrix C comprises:

determining two permutation matrices $P_1, P_2 \in Z_2^{k \times k}$ such that all codewords in an [2k,k,d] error-correcting code, represented by the generator matrix (I_k || P_1 C P_2), have a predetermined multi-bit weight; and

using P_1 C P_2 as the matrix A.

13. (Previously presented) A system as claimed in claim 12, wherein the input block data is m-bit sub-block data, and the processing apparatus executes a round function with an S-box layer with S-boxes operating on the m-bit sub-block data, and the minimum predetermined multi-bit weight over all non-zero codewords equals a predetermined m-bit weight.

14. (Previously presented) A system as claimed in claim 12, wherein determining the two permutation matrices P_1 and P_2 comprises iteratively generating the matrices in a random manner.

15. (Previously presented) A system as claimed in claim 8, wherein the input data block is a 32-bit data block and wherein the operation of generating a [n,k,d] error-correcting code comprises:

generating a binary extended Bose-Chaudhuri-Hocquenghem (XBCH) [64,36,12] code; and

shortening the XBCH [64, 36, 12] code to a [60, 32, 12] XBCH code by deleting four rows.

PAGE 7/12 * RCVD AT 8/14/2006 3:55:34 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/28 * DNIS:2738300 * CSID:703 5199802 * DURATION (mm-ss):01-56

16. (Previously presented) A method of linear transformation in a symmetric-key cipher comprising:

inputting block data into a processing apparatus;

creating a linear transformation matrix A with the processing apparatus by:

generating a binary [n,k,d] error-correcting code, represented by a generator matrix $G \in Z_2^{k \times n}$ in a form $G = (I_k \| B)$, with $B \in Z_2^{k \times (n-k)}$, where $k < n < 2k$, and d is the minimum distance of the binary error-correcting code;

extending matrix B with 2k-n columns such that a resulting matrix C is non-singular;

determining two permutation matrices $P_1, P_2 \in Z_2^{k \times k}$ such that all codewords in an [2k,k,d] error-correcting code, represented by the generator matrix $(I_k \| P_1 C P_2)$, have a predetermined multi-bit weight; and

using $P_1 C P_2$ as matrix A; and

transforming the input block data into diffused output block data with the processing apparatus by using the linear transformation matrix A.

PAGE 8/12 * RCVD AT 8/14/2006 3:55:34 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/28 * DNIS:2738300 * CSID:703 5199802 * DURATION (mm-ss):01-56